Module One

The Need for Trusted Systems

This module describes why trusted systems are needed and how this needhas led to the development and evolution of the Trusted Computer System Evaluation Criteria (TCSEC) [TCSEC85] and the Trusted ProductEvaluation Program (TPEP). The module describes the basic requirements forsecrecy , integrity, and availability of information assets. It discusses threats to, and vulnerabilities of, computer systems, and describes countermeasures to these threats and vulnerabilities. Additional basic topics introduced include security policies, mechanisms, and models; the trusted computing base; and security disciplines and risk management.

The TCSEC is then introduced and briefly described, including its purpose, its contents, and how it is used. Finally, the TPEP is introduced, including paragraphs on the Evaluated Products List (EPL) [ISSP94] and theneed for rating maintenance.

Module Learning Objectives

The material presented in this module should be read prior to readingmaterial in any other module. The objective of this module is to introduce the fundamental concepts of information protection in computing systems thatwill serve as a basis for security concepts presented in subsequent coursemodules . Upon completion of this module, the student should:

1. Understand the need for trusted systems.
2. Understand the history and future direction of trusted systems criteria development.
3. Understand the fundamental concepts and terminology of information protection.
4. Be familiar with the structure and use of the TCSEC.
5. Be aware of the Trusted Product Evaluation Program.

Overview

This module establishes the foundation for understanding the information presented in the remaining modules. Modules 2-3 address the role of computer security in the context of U.S. government organizations and policies. Modules 4-16 address security requirements in the TCSEC that are primarilydirected at operating systems. TNI Modules 1-4 address interpretations of TCSEC requirements in the Trusted Network Interpretation (TNI) [TNI87]that are directed at networks. TDI Modules 1-4 address interpretations of TCSEC requirements in the Trusted Database Interpretation (TDI) [TDI91]that are directed at databases and other applications.

This module begins with a brief history of the evolution of the TCSEC, the TPEP, and more recent trusted systems criteria efforts. This history is followed by a discussion of fundamental computer security concepts and terminology. An overview of the TCSEC is given next, and the module ends with anoverview of the process by which National Security Agency (NSA) representatives evaluate trusted products (i.e., TPEP).

History

In October 1967, a task force was assembled by the Defense Science Board to address computer security safeguards that would protect classified information in remote-access, resource-sharing computer systems. More and more, computers were becoming a necessary element of the efficient operationof society. It became evident that there was a need to have the technology and the know-how to operate computers and communications systems in a secure manner while continuing to expand the available resources and make interconnections more flexible. The Task Force report [Ware70] led to a number of efforts sponsored by the Department of Defense (DoD) and theNational Bureau of Standards, now the National Institute for Standards and Technology (NIST), to define problems and solutions for building andevaluating secure computer systems. As an outgrowth of these efforts, work began on an initial set of computer security evaluation criteria that could be used to assessthe degree of trust one could place in a computer system to protect sensitivedata [Nibaldi79a, Nibaldi79b, Trotter80]. The preliminary concepts for computer security evaluation were subsequently defined, expanded upon, andsubjected to extensive peer review by computer security experts from industry, academia, and the U.S. government.

The DoD Computer Security Center was formed in January 1981 to staff and expand on the work started by the DoD [Faurer81]. The name was changed to the National Computer Security Center (NCSC) in December 1985. Amajor goal of the NCSC as given in its DoD Charter is to encourage thewidespread availability of trusted computer products for use by those who process classified or other sensitive information. The NCSC's fundamental approach was to produce generic requirements that could be used by any vendor tobuild trusted products, but that would also serve as standardized criteria for evaluating the trust classes of those products. The assumption was that "if they were built, they could be evaluated -- and if evaluated, they would bebought. " The NCSC used the initial set of evaluation criteria cited above as abasis for producing the TCSEC, and developed TPEP based on the preliminary concepts of evaluation refined by computer security experts.

The TCSEC was published in 1983 in the now familiar orange cover. The "Orange Book" underwent a minor revision and was declared a DoD standard, DoD 5200.28-STD, in 1985, and has remained unchanged with the exception of necessary Interpretations. Interpretations are written to clarify issues that are not explicit in the general TCSEC requirements. Three of the Interpretations are in their own separate documents (i.e., TNI, TDI, Computer Security Subsystem Interpretation [CSSI88]), and the rest are publishedannually in [INTERP94]. Although Interpretations are often incorrectly seen as ameans of increasing the original requirements (colloquially termed "CriteriaCreep"), they are actually intended to address issues that have not been considered before (e.g., new designs, new technologies).

Other trusted system criteria efforts have been and/or are being undertaken to address perceived shortcomings in the TCSEC. The four primary efforts are the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) [CTCPEC93], the Information Technology Security Evaluation Criteria (ITSEC) [ITSEC91], the Federal Criteria, and the Common Criteria. The

CTCPEC was developed by Canada and first published in 1989. The ITSEC was developed jointly by a number of European countries and firstpublished in 1990. The Federal Criteria effort was undertaken by the U.S. starting in 1992 as a reworking of the TCSEC, but no document was ever officially published. Instead, the Federal Criteria effort transitioned to become input, along with the CTCPEC and ITSEC, into the Common Criteria being jointly developed by the U.S., Canada, and Europe. The Common Criteria expands the scope of trusted system criteria to address areas such as distributed systems and cryptography. This effort is currently in progress, so the TCSEC is still the standard that is used today and is the focus of discussion in the remainder of this course.

Fundamental Computer Security Concepts and Terminology

This section presents concepts and terminology that are fundamental to understanding protection in computer systems. These fundamentals form the foundation for this course and for investigating more advanced computer security material. Students are encouraged to read [Saltzer75], afoundational paper containing greater detail on computer security fundamentals.

Confidentiality, Integrity, and Availability

Computer security addresses three principal needs: confidentiality, integrity, and availability. *Confidentiality*, or secrecy, involves preventing unauthorized disclosure of information. *Integrity* involves preventing unauthorized changes to information or information resources. *Availability* involves preventing the unauthorized delay or denial of use of information and resources.

The TCSEC requirements focus on preventing unauthorized disclosure because the DoD was initially most concerned with confidentiality. Data and systems integrity is a primary concern for commercial organizations andis receiving more emphasis in the DoD. While theoretical work has evolved to show promise of describing enforceable and useful data and systemsintegrity principles [Biba77, Clark87, Mayfield91], there remains no explicit criteria for evaluating systems that enforce integrity. Theoretical work on availability has begun [Gligor83, Yu88, Millen93], but there is little basis for evaluating a system against an availability requirement.

Vulnerabilities, Threats, and Countermeasures

Security is traditionally discussed in terms of vulnerabilities, threats, and countermeasures. A *vulnerability* is some aspect of a system that leaves it open to attack. A *threat* is a party with the potential to exploit one or more vulnerabilities and cause damage. A *countermeasure*, or safeguard, is an added step or improved design that eliminates a vulnerability and renders athreat impotent. [Schell79] presents an excellent treatise on the potential threats to DoD systems, the inherent vulnerabilities of typical computer systems, and the fundamentals of trust technology.

Vulnerabilities can be related to procedures (e.g., open connection to a network), personnel (e.g., uneducated user), systems (e.g., design error), or the environment (e.g., located in enemy territory). Threats can be accidental (e.g., human error) or malicious (e.g., hacker, malicious software [Thompson83]), and can be directed at compromising confidentiality (e.g., eavesdropping on communication channels, browsing through files, reading memory segments that have not been erased), integrity (e.g., tampering, message reordering, data entry errors), or availability (e.g., jamming a communications channel, crashing the system). Countermeasures consist of policies, mechanisms, and models as described below.

Policies, Mechanisms, and Models

Security policies specify the rules that govern how information is to be protected; *security mechanisms* (administrative, procedural, and technical) enforce the policies. Policies are distinguished from mechanisms because a given policy may be enforced by different types of mechanisms, and a given mechanism may enforce several policies. *Security models* precisely and unambiguously represent a security policy. For example, the Bell and La Padula Model -- Multics Interpretation [Bell76] represents the DoDsecurity policy for classified information on a shared-resource system. Security models, policies and mechanisms are described in more detail in Module 5.

Most security countermeasures fall into one of six categories: accesscontrols , object reuse, identification and authentication (I&A), audit, assurance, and cryptography. Each of these categories is described below.

- Access controls ensure that the reading, changing, and deleting of data and programs is authorized. They can be modeled by a matrix that specifies the access rights permitted by a policy. The rows of the matrix are *subjects*, which are the active entities that access information assets. Subjects may correspond to users or to processes operating on behalf of users. The columns of the matrix are *objects*, which are the passive information assets to be protected. Objects may correspond to files, devices, or views on a database. The entries inside the matrix are the access rights (e.g., read, write) that have been granted to a given subject with respect to a given object. Mandatory access control (MAC) policies and mechanisms implement rule-based, system-wide administrative control over *all* objects; MAC is described in Module 8. Discretionary access control (DAC) policies and mechanisms implement identity-based, owner-only control over *selected* objects; DAC is described in Module 9.
- Object reuse involves preventing the unauthorized disclosure of residual data after an object has been deleted. Object reuse policies and mechanisms are described in Module 10.
- I&A provides the ability for a system to validate the identity of auser or for a system and a user to mutually validate each other before processing begins. I&A policies and mechanisms are described in Module 11.
- Auditing provides accountability by recording users’ actions into a log that is available for future review. Audit policies and mechanisms are described in Module 12.

- Assurances provide confirmation that the protection features are operating as intended. Assurance policies and mechanisms are described in Modules 13-15.
- Cryptography protects information from unauthorized disclosure and undetectable, unauthorized modification by encrypting plaintext data into ciphertext at the sender and decrypting ciphertext back into plaintext data at the receiver. Cryptography policies and mechanisms are described in TNI Module 4.

Trusted Computing Base

The *trusted computing base (TCB)* consists of the totality of protection mechanisms responsible for enforcing a protection policy within a computer system. A TCB includes hardware, firmware, and operating system software. The critical part of a TCB is called the reference monitor [Anderso72]. A *reference monitor*, or security kernel as it is sometimes called, is a subset of the TCB whose task is to check the legitimacy of each attempt by a subject to access an object. A reference monitor must be tamperproof, must always be invoked, and must be small enough and simple enough to be thoroughly understood.The reference monitor and TCB are described in Module 6. Architecture and design requirements for the TCB are described in Module 7.

Security Disciplines and Risk Management

Operating a computer system securely requires a multi-disciplinedapproac h. Each of the following interrelated *security disciplines* contribute to the overall security of an operational system.

- Physical Security
- Administrative Security
- Personnel Security
- Communications Security
- Emanations Security
- Hardware & Software Security

Risk management strikes a balance among the security disciplines to ensure that a system in an operational environment can accomplish its missionwhile achieving an acceptable level of risk. Risks arise because an attack could exploit some system vulnerability. That is, each vulnerability of a system reflects a potential threat, with corresponding risks [Clark91]. Sinceit is neither technically nor fiscally possible to build a system that is completely secure (and still useful), there will always be some amount of risk. Threats and vulnerabilities are identified and countermeasures from each of the security disciplines are applied to reduce the risk to an acceptable level. The“Y ellow Book” [ENV85] can be used to guide the selection of an appropriate TCBfor a given environment.

Computer security, like a chain, is only as strong as the weakest link. In order to provide a secure operating environment, each of the security disciplines must be addressed uniformly. The TCSEC addresses only the hardware and software security issues; [ISSO92] provides guidance to Information System Security Officers that also addresses the other areas. The remainder of this module is comprised of overviews of the TCSEC and the TPEP.

Overview of the TCSEC

The purpose of the TCSEC is three-fold. First, it presents a consistent set of DoD computer security requirements (as opposed to specifications)that can be used as a standard for commercial development of trusted products. Second, it aids DoD Components in understanding the degree of trust that may be placed in computer systems. Finally, it provides a basis for specifying security requirements in acquisition specifications. This final purpose was found to be a weak link, so a four-volume set of procurement guidelines was developed to clarify how to use the TCSEC in the acquisition of trusted systems [PROC94].

This section identifies the TCSEC security policy and describes thecontrol objectives derived from this policy. The hierarchy of TCSEC requirements is then briefly described. The section concludes with a discussion of TCSEC Interpretations.

TCSEC Security Policy and Control Objectives

The TCSEC security policy forms the basis for deriving control objectivesto be used in implementing protection in computing systems. This policy is derived from the following DoD documents:

- Executive Order 12356 [NSI82] -- States the national requirements for classification, declassification and safeguarding of national security information.
- OMB Circular A-130 [MFIR94] (supersedes OMB Circular A-71) -- Directs establishment and maintenance of a computer security program within each branch of the Government.
- DoD Regulation 5200.1-R [ISPR87] -- Establishes and defines security within DoD.
- DoD Directive 5200.28 [AIS88] and DoD Manual 5200.28-M [ADPSM79] -- Dictate the control objectives for ADP security.

Control objectives provide a fundamental framework for developing astrategy to satisfy security requirements for any system. An overview is givenbelow , and a more detailed discussion of control objectives can be found inChapter 5 of the TCSEC [TCSEC85]. There are three primary control objectives:security policy, accountability, and assurance.

Security Policy Control Objective

The security policy control objective requires that a security policy bedefined and shown to be correctly implemented for any system processing sensitive information. A security policy is a precisely defined statement ofintent with regard to the control over access to and dissemination of information.This control objective is further subdivided into three sub-objectives:mandatory security policy, discretionary security policy, and marking.

The Mandatory Security Policy Control Objective states that access must be controlled based directly on a comparison of an individual's clearance and the classification of the information being sought. Clearances and classifications include hierarchical levels and non-hierarchical categories. DoD mandatory security is mathematically a lattice model. Within a single compartment, the classification levels are hierarchical. For example, eligibility to access the Secret level automatically gives you eligibility to access theConfidential and Unclassified levels, but not the Top Secret level. The model is only partially ordered in that there is no relationship between compartments. Eligibility to access a particular compartment does not permit eligibility to accessany other compartment. The DoD mandatory security policy control objective isderived from:

- Executive Order 12356 [NSI82] -- Requires that eligibility for access must be based on a determination of trustworthiness.
- DoD Regulation 5200.1-R [ISPR87] -- Establishes a Special Access Program (formal need to know), and states that trustworthiness means clearance.
- DoD Manual 5200.28-M [ADPSM79] -- Requires that system developers and maintainers must have clearances.

The Discretionary Security Policy Control Objective states that access to objects must be controlled to limit access based on identifiedindividuals who have been determined to have a need to know for the information. Discretionary controls are not explicitly controlled by regulation; theyare controlled by the individual users (i.e., they are informal need-to-know controls). They are not a replacement for mandatory controls, but a supplement that provides necessary additional security control. The DoDdiscretionary security policy control objective is derived from:

- DoD Regulation 5200.1-R [ISPR87] -- Requires that no person may have access to classified information unless access is necessary for performance of official duties.

The Marking Control Objective states that systems must store andpreserve the integrity of classification and sensitivity labels for all information. Labels exported from the system must be accurate representations of theinternal labels. Marking (or labeling) is necessary to implement mandatory access controls. Without accurate identification of the sensitivity label of subjectsand objects, correct access decisions cannot be made. The DoD marking control objective is derived from:

- Executive Order 12356 [NSI82] -- Requires that classification markings be shown on the face of all classified documents.
- DoD Regulation 5200.1-R [ISPR87] -- Requires that new ADP systems will provide internal labels, and produced documents will have external labels.

Accountability Control Objective

The accountability control objective requires the system to ensureindividual accountability whenever a mandatory or discretionary policy is invoked.The capability must exist for an authorized agent to access and evaluate accountability information by a secure means, within a reasonable amount of time, and without undue difficulty. Key aspects of the accountability control objective are I&A and audit. The DoD accountability control objective is derived from:

- DoD Directive 5200.28 [AIS88] -- Requires that each user's identity be positively established, and his access and activities controlled and open to scrutiny.
- DoD Manual 5220.22-M [ISM91] -- Requires that systems provide audit trails tracking: personnel access, start/stop time of classified processing, all functions initiated by system operators, disconnects of remote terminals, log-on and log-off user activity, unauthorized attempts to access files or programs (as well as all authorizedopen, close, create, and file destroy actions), and program aborts and anomalies.

Assurance Control Objective

The assurance control objective requires the system to be designed so asto guarantee correct and accurate interpretation of the security policy. Assurance must be provided that the correct implementation and operation of thepolicy exists throughout the system's life-cycle. Two types of assurance are needed: life-cycle and operational. Life-cycle assurances are the steps taken to ensure that the system is designed, developed, and maintained using formalizedand rigorous controls and standards to protect against unauthorized changes to the system; configuration management is a key aspect of life-cycle assurance. Operational assurance focuses on features and system architecture used to ensure that the security policy is uncircumventably enforced duringsystem operation; testing and isolation of protection critical code are examplesof operational assurance. The DoD assurance control objective is derived from:

- DoD Directive 5200.28 [AIS88] -- Requires that security policies, concepts and measures shall be considered from the beginning of the design.
- DoD Manual 5200.28-M [ADPSM79] -- Requires that testing will be done throughout the lifetime to maintain a secure system.
- DoD Directive 5215.1 [CSEC81] -- Requires evaluations of industry and government developed trusted computer systems against these criteria.

TCSEC Requirements Hierarchy

This section gives an overview of the hierarchical divisions and classes in the TCSEC. Divisions range from A-D, and classes are designated by numerical values within a division. When evaluating a product against the TCSEC, the product is assigned a rating of the highest class for which it satisfies *all* of the requirements. The possible ratings, from lowest to highest, are: D, C1, C2, B1, B2, B3, A1.[1] The requirements mentioned in general here will be explained and expanded upon in greater detail in subsequent modules. In particular, a requirement-by-requirement description is given in Module 4.

The TCSEC combines two types of security requirements: features and assurances. Features are specific functional capabilities required in a trusted computer product, and assurances are actions taken to gain confidencethat the required features are actually present and operating as intended. Thelower classes of the TCSEC (B1 and below) concentrate on features. There is a gradual shift from adding features to adding assurances in the higher classes (B2 and above).

Minimal Protection: Division D

Division D is in some sense a catch-all. A product given a D rating may simply fail to meet all the requirements for a higher class and may still offer some useful security features.

Discretionary Protection: Division C

Division C provides protection features to support cooperating users atthe same sensitivity label. Discretionary protection could be likened topersonal ownership, in that it is at the discretion of the owner of the data to grantother people access to the data. Products in this division provide fordiscretionary protection and, through inclusion of audit capabilities, for accountability of subjects and the actions they initiate. Division C is divided into two classes, the primary distinction between the classes being the granularity of the discretionary controls.

Class C1 products provide nominal discretionary security protection by separation of users and data. They provide access limitations by named individuals or defined groups or both. However, the product need not be able to associate system users with unique individuals.

Class C2 products must be able to uniquely identify individual users ofthe system and hold them accountable for their actions. Users are individually accountable for actions through login procedures, auditing, and resource isolation.

Mandatory Protection: Division B

Division B introduces the use of sensitivity labels and uses them toenforce a set of MAC rules in addition to the discretionary controls of Division C. In addition to increased security functionality, there are dramatically increasing requirements for assurance that the protection features functioncorrectly . Division B is divided into three classes.

[1] Note that subsystems receive ratings of D1, D2, or D3 by meeting aparticular subset of the TCSEC requirements in a given class. D1 is assigned to a subsystem that meets a particular subset of the C1 requirements, D2 is assigned to a subsystem that meets a particular subset of the C2 requirements, and D3 is assigned to a subsystem that meets a particular subset of theB3 requirements [CSSI88].

Class B1, Labeled Security Protection, is the first class at which the product has knowledge of the classification of the information and the clearances associated with users. Sensitivity labels are associated with named subjects and objects. Numerous other features are added or extended to make use of these labels, for example, I&A, auditing, and MAC. Stronger assurance measures are prescribed due to the increased potential of compromisefrom use in higher threat environments. This class introduces the use of formal assurance techniques (the requirement for a security policy model) in addition to the classical testing required at Division C.

Class B2, Structured Protection, represents a major step up architecturally. At this class, you have implemented the basic requirements for a reference monitor. Labels are now associated with all subjects and objects in the system, and the MAC mechanism is extended to support them. The I&A function is also strengthened by the added requirement for a trusted path. Many more assurance activities are required to satisfy the trust necessary at thisc lass. These include: a formal security policy model, covert channel analysis, a descriptive top-level specification and substantially more securitytesting . Configuration management is required beginning at this class to establish and maintain the high degree of trust in the product throughout its life-cycle.

Class B3, Security Domains, can be viewed architecturally as a refinement of the B2 architecture requirements. The architecture now represents a clean implementation of the reference monitor concept. Only security critical functionality exists within the TCB. There are also several minor changes and additions to the protection feature requirements. For example, the discretionary policy is extended to specifically require access controllists , and to be able to explicitly deny access to objects by named individuals orgroups . Others include extensions to the trusted path and the audit requirements, and new requirements for a separate security administrator function andtrusted recovery mechanism. The assurance requirements are increased in the analysis and test of the protection mechanism.

Verified Protection: Division A

At Division A there are no additional feature requirements. This division is characterized by the use of formal verification methods to assure thatthe specific security feature requirements in the product can effectivelyprotect classified or other sensitive information stored or processed in thesystem. Division A has only one class.

Class A1, Verified Design, is functionally equivalent to Class B3. All of the additional effort spent to achieve Class A1 is directed at increasing the level of assurance, through the application of formal methods. This additional effort includes: formal specification and verification of the security design,covert channel analysis, and manual or other mapping of the formal specification to the source code. In addition, requirements for configuration management are strengthened and a new requirement for trusted distribution is introduced.

TCSEC Interpretations

A TCSEC Interpretation (or “interp”) is an interpretation ofa requirement(s) in the TCSEC. Interps are, in effect, amendments or additions to the TCSEC. They serve to clarify or explain a part of the TCSEC. All products under evaluation must meet all the Interpretations in effect at the time theformal phase of that evaluation begins. A more detailed discussion of the Interpretations Process can be found in Module 4.

Trusted Product Evaluation Program

NSA’s evaluation program, TPEP, is focused on the technical evaluation of the protection capabilities of off-the-shelf, commercially produced and supported products against the TCSEC. It is an open process where the developer knows in advance the basis of the evaluation and is a participant in theprocess . The intent of the evaluation program is to make trusted products widely available within DoD and industry. TPEP consists of three phases (Pre-Evaluation, Evaluation, and RAMP) as described in detail in Module 4.

An *evaluation* is performed by NSA representatives independent of a product’s intended operational environment. The results of an NSA evaluation canbe used as inputs into a system *certification* process performed by various agencies. Formal *accreditation* remains the ultimate responsibility of a Designated Approving Authority. Module 2 describes the concepts of evaluation, certification, and accreditation in more detail.

NSA performs four types of product evaluations: operating system,network component, database, and subsystem. NSA evaluates products that address all the requirements of a given class of the TCSEC and include everything needed to accomplish a job, end user to end user. A network component is a trusted building block which can be used as part of a complete trusted system. Network components can provide any of a large range of security services (e.g., communication backbone between workstations, gateway, file server). NSA evaluates network components against the TCSEC as further defined in [TNI87]. A secure database is a database management system that has been designed and built to meet a class of the TCSEC as further defined in [TDI91]. Subsystems are special-purpose products that can be added to existing computer systems to increase security and implement only a subset ofsecurity features identified in the TCSEC (i.e., audit, object reuse, DAC, I&A). Subsystem products are evaluated against the TCSEC as further definedin [CSSI88].

Evaluated Products List

An entry in the EPL results from each completed evaluation. An EPL entry consists of an executive summary of the security features and the ratingof the product. The EPL entry is posted in the **Announce** meeting on Dockmaster as soon as the summary is completed, reviewed for proprietary information,and approved for public release. Each quarter, NSA publishes [ISSP94], which includes the EPL, information about ongoing NSA evaluation activities, and information about other NSA endorsed security products (e.g., cryptographic equipment, TEMPEST equipment).

Rating Maintenance Phase

As an introduction, RAMP was instituted to extend the ratings of trusted products on the EPL to current releases of the products. Once a product receives a rating from NSA, RAMP levies much of the responsibility for continued trust analysis and maintenance on the vendor. Configuration controls are required of the vendor to capture the trail of evidence ofcontinued trust for presentation to NSA. A more detailed discussion of RAMP can be found in Module 16.

Relevant Trusted Product Evaluation Questionnaire Questions

None.

Required Readings

TCSEC85 National Computer Security Center, *Department of Defense Trusted Computer System Evaluation Criteria*, DoD 5200.28-STD, December 1985.

The entire TCSEC should have been read prior to beginning this course. The Preface and the Introduction describe the history of computer security; the purpose, scope and structure of the TCSEC; and the fundamental requirements of computer security. Chapter 5 describes the control objectives for trusted computer systems. Chapter 6 discusses the rationale behind the evaluation classes. Chapter 7 documents the relationship between DoD policy and the TCSEC. Appendix A should be ignored because it describes an outdated evaluation process. Appendices B and C summarize the division and class designations of the TCSEC. The other chapters of the TCSEC will be required and tested in later modules.

Gasser88 Gasser, M., *Building a Secure Computer System*, Van Nostrand Reinhold Co., N.Y., 1988.

The entire book should have been read prior to beginning this course. Chapter 1 describes what security is, and Chapter 2 explains why most systems are not secure.

Schell79 Schell, R.R., “Computer Security: The Achilles’ Heel of the Electronic Air Force?,” *Air University Review*, Vol. 30, No. 2, January 1979.

This paper describes the classical vulnerabilities of computer systems, discusses the need to design security into the system from the outset, and introduces the reference monitor concept.

Supplemental Readings

CSSI88 National Computer Security Center, *Computer Security Subsystem Interpretation of the TCSEC*, NCSC-TG-009, Version 1, 16 September 1988.

This document describes the evaluation of products that have been designed and built to satisfy only a subset of the TCSEC requirements at a given class (e.g., I&A).

ENV85 DoD Computer Security Center, *Guidance for Applying the DoD TCSEC in Specific Environments*, CSC-STD-003-85, June 1985.

INTERP94 National Computer Security Center, *The Interpreted TCSEC Requirements*, (quarterly).

ISSO92 National Computer Security Center, *A Guide to Understanding Information System Security Officer Responsibilities for Automated Information Systems*, NCSC-TG-027, Version 1, May 1992.

PROC94 National Security Agency, *A Guide to Procurement of Trusted Systems*, NCSC-T9-024, Version 1, Vols. 1-4, February 1994.

TNI87 National Computer Security Center, *Trusted Network Interpretation of the TCSEC*, NCSC-TG-005, Version 1, July 1987.

This document interprets the TCSEC for the evaluation of products that have been designed and built to satisfy the TCSEC requirements in a network environment.

TDI91 National Computer Security Center, *Trusted Database Management System Interpretation of the TCSEC*, NCSC-TG-021, Version 1, April 1991.

This document interprets the TCSEC for the evaluation of database products and other applications that have been designed and built to satisfy the TCSEC requirements.

<u>Other Readings</u>

ADPSM79 Department of Defense, *ADP Security Manual -- Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource-Sharing ADP Systems*, DoD 5200.28-M, June 1979.

AIS88 Department of Defense, *Security Requirements for Automated Information Systems*, DoD 5200.28, March 1988.

Anderso72 Anderson, J.P., *Computer Security Technology Planning Study*, ESD-TR-73-51, Vol. I, AD-758 206, ESD/AFSC, Hanscom AFB, Bedford, MA, October 1972.

Boebert85 Boebert, W.E. and Kain, R.Y., “Secure Computing: The Secure Ada Target Approach,” *Scientific Honeyweller*, Vol. 6, No. 2, pp. 1-17, July 1985.

Bell76 Bell, D.E. and La Padula, L.J., *Secure Computer Systems: Unified Exposition and Multics Interpretation*, MTR-2997, Rev. 1, MITRE Corporation, Bedford, MA, March 1976.

Biba77 Biba, K.J., *Integrity Considerations for Secure Computer Systems*, MITRE Corporation, Bedford, MA, 1977.

Clark87 Clark, D.D. and Wilson, D.R., “A Comparison of Commercial and Military Computer Security Policies,” *Proceedings of the 1987 IEEE Symposium on Security and Privacy*, pp. 184-194, May 1987.

Clark91 National Research Council (Clark, D.D., et. al.), *Computers at Risk -- Safe Computing in the Information Age*, National Academy Press, 1991.

CSEC81 Department of Defense, *Computer Security Evaluation Center*, DoD 5215.1, 1981.

CTCPEC93 Canadian System Security Centre, *The Canadian Trusted Computer Product Evaluation Criteria*, Version 3.0e, January 1993.

Denning79 Denning, D.E. and Denning, P.J., “Data Security,” *Computing Surveys*, Vol. 11, No. 3, pp. 227-249, September 1979.

Faurer81 Faurer, L.D. “Keeping Secrets Secret,” *Government Data Systems*, pp. 14-17, November-December 1981.

Gligor83 Gligor, V.D., “A Note on the Denial of Service Problem,” *Proceedings of the 1983 IEEE Symposium on Security and Privacy*, pp. 139-149, April 1983.

ISM91 Department of Defense, *Industrial Security Manual for Safeguarding Classified Information*, DoD 5220.22-M, January 1991.

ISPR87 Department of Defense, *Information Security Program Regulation*, DoD 5200.1-R, April 1987.

ISSP94 National Security Agency, *Information Systems Security Products and Services Catalog*, GPO 908-027-00000-1, (quarterly).

ITSEC91 Commission of the European Communities, *Information Technology Security Evaluation Criteria*, Version 1.2, June 1991.

Mayfield91 National Computer Security Center (Mayfield, W.T., et. al.), *Integrity in Automated Information Systems*, C Technical Report 79-91, September 1991.

MFIR94 Office of Management and Budget, *Management of Federal Information Resources*, OMB Circular A-130, July 1994.

Millen93 Millen, J.K., “A Resource Allocation Model for Denial of Service Protection,” *Journal of Computer Security*, Vol. 2, Nos. 2&3, pp. 89-106, 1993.

Nibaldi79a Nibaldi, G.H., *Proposed Technical Evaluation Criteria for Trusted Computer Systems*, M79-225, AD-A108-832, MITRE Corporation, 25 October 1979.

Nibaldi79b Nibaldi, G.H., *Specification of a Trusted Computing Base (TCB)*, M79-228, AD-A108-831, MITRE Corporation, 30 November 1979.

NSI82 President of the United States, *National Security Information*, E.O. 12356, 6 April 1982.

Pfleeger89 Pfleeger, C.P., *Security in Computing*, Prentice Hall, N.J., 1989.

Saltzer75 Saltzer, J.H. and Schroeder, M.D., "The Protection of Information in Computer Systems," *Proceedings of the IEEE*, Vol. 63, No. 9, pp. 1278-1308, September 1975.

Thompso83 Thompson, K., "Reflections on Trusting Trust," *ACM Turing Award Lectures, The First Twenty Years, 1966-1985*, ACM Press, NY, pp. 171-177, 1987.

Trotter80 Trotter, E.T. and Tasker, P.S., *Industry Trusted Computer Systems Evaluation Process*, MTR-3931, MITRE Corporation, 1 May 1980.

Ware70 Ware, W.H., ed., *Security Controls for Computer Systems: Report of the Defense Science Board Task Force on Computer Security*, AD-A076617/0, Rand Corporation, February 1970 (reissued October 1979).

Yu88 Yu, C. and Gligor, V.D., "A Formal Specification and Verification Method for the Prevention of Denial of Service," *Proceedings of the 1988 IEEE Symposium on Security and Privacy*, pp. 187-202, April 1988.